REMARKS/ARGUMENTS

Claims 1-22 are pending in the present application. Claims 1- 4, 6, 7-11, 15-18, and 22 were amended. Claims 4, 6, 11, and 18 were amended to correct informalities and not in response to any art rejections. These amended claims have not changed in scope with respect to whether the claims are patentable over the cited references. No claims have been added or canceled. Support for the amendments to the claims may be found in the Specification at least on page 12, lines 18-page 14, line 8, page 13, lines 19-28, page 17, line 6-page 18, line 10, and **Figure 5,** reference numbers 506-520. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 112, Second Paragraph

The examiner has rejected claims 4 and 6 under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter, which applicants regard as the invention. This rejection is respectfully traversed.

With regards to the objected claims, the Examiner states:

> Claim 4 recites the limitation "the granting step". There is insufficient antecedent basis for this limitation in the claim.
> Claim 6 recites the limitation "the generating step". There is insufficient antecedent basis for this limitation in the claim.

Office Action dated November 06, 2006, Page 2.

Claim 4 has been amended to recites "wherein granting a security identifier given by the access control list to the process further comprises...." Claim 6 has been amended to recite "wherein generating the access decision based on the security identifier further comprises...." There is sufficient antecedent basis for these limitations in claim 1. Therefore the rejection of claims 4 and 6 under 35 U.S.C. § 112, second paragraph has been overcome.

II. 35 U.S.C. § 102, Anticipation

The examiner has rejected claims 1-22 under 35 U.S.C. § 102(b) as being anticipated by *Benson et al.*, Providing Secure Access for Multiple Processes Having Separate Dirrectories, U.S. Patent No. 5,867,646 (February 02, 1999) (hereinafter *US '646*). This rejection is respectfully traversed.

With regards to claims 1, 8, 15 and 22, the Examiner states:

> For claim 1 and similar claims 8, 15 and 22, US '646 discloses a method and apparatus for data processing system for managing access to resources, the method and apparatus comprising: granting a process a security identifier, wherein the security identifier has no meaning outside of being used to make an

> access decision for a specific resource; and responsive to the process requesting access to the specific resource, generating the access decision based on the security identifier. (see Abstract; Figure 2; column 1, line 52 - column 2, lines 1 - 30)

Office Action dated November 06, 2006, Page 3.

A prior art reference anticipates the claimed invention under 35 U.S.C. § 102 only if every element of a claimed invention is identically shown in that single reference, arranged as they are in the claims. *In re Bond*, 910 F.2d 831, 832, 15 U.S.P.Q.2d 1566, 1567 (Fed. Cir. 1990). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). Anticipation focuses on whether a claim reads on the product or process a prior art reference discloses, not on what the reference broadly teaches. *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 218 U.S.P.Q. 781 (Fed. Cir. 1983). Applicants respectfully submit that *Benson* does not teach granting a security identifier given by an access control list to a process in response to matching an entry in an access control list of a specific resource with credentials of a process.

Claim 1, which is representative of other rejected claims 8, 15, and 22 with respect to similarly recited subject matter, reads as follows:

> 1. A method in a data processing system for managing access to resources, the method comprising:
> responsive to matching an entry in an access control list of a specific resource with credentials of a process, granting a security identifier given by the access control list to the process, wherein the security identifier has no meaning outside of being used to make an access decision for the specific resource; and
> responsive to the process requesting access to the specific resource, generating the access decision based on the security identifier.

Applicants respectfully submit that *Benson* does not teach each and every feature in amended claim 1 in the same arrangement as is recited in claim 1. More specifically, *Benson* does not teach "responsive to matching an entry in an access control list of a specific resource with credentials of a process, granting a security identifier given by the access control list to the process, wherein the security identifier has no meaning outside of being used to make an access decision for the specific resource," as is claimed in claim 1. *Benson* is directed toward providing a directory of process-specific identifiers. In *Benson*, a user may gain access to a process if the user's system identifier is associated with a desired process-specific identifier. *Benson* states:

> A variety of processes, e.g., electronic mail, word processing, database applications, etc., reside on a system, e.g., an operating system. Independent levels of security are

maintained for the different processes without requiring the user to pass a security test to gain access to each process. The system includes a directory of system identifiers assigned to users. Each process includes a directory of process-specific identifiers for users of that process. The system identifiers and process identifiers are associated in a predetermined manner. Therefore, a user may gain access to a process only when the user's system identifier is associated with the desired process-specific identifier.

Benson, Abstract.

As shown above, *Benson* a user is allowed to gain access to a variety of processes without requiring the user to pass a security test, such as entering a password, to gain access to each process. However, *Benson* does not teach granting a security identifier given by an access control list of a specific resource to a process in response to matching an entry in the access control list with credentials of the process. In fact, *Benson* does not even mention granting a security identifier or an access control list in this or any other section of the reference.

The system identifier and process-specific identifiers of *Benson* are not equivalent to the security identifier of claim 1. *Benson* teaches that when a user attempts to access an operating system or resource, the user must have an authorized system identifier. *Benson* states:

> In one embodiment, a first process is an operating system which includes an associated security system for controlling access to the operating system. The operating system includes a directory of system identifiers which represent the authorized users. Therefore, when a user attempts to access the operating system, the user must have an authorized system identifier and must pass an explicit security test.

Benson, column 1, lines 59-67.

As shown above, *Benson* seems to assume the user already has already been assigned a system identifier. (*See Benson* at column 3, lines 4-6.) *Benson* does not provide any teaching for how this identifier is assigned. Moreover, *Benson* does not teach assigning or granting a system identifier, or any other identifier, to a user or a process in response to matching an entry in an access control list with credentials of a process or in response to performing any other matching operation. Moreover, as mentioned above, *Benson* does not even mention an access control list. Therefore, it would not be possible for *Benson* to grant an identifier based on an entry in an access control list.

Benson also fails to teach granting a security identifier in response to **matching** an entry in an access control list of a specific resource with credentials of a process, as is claimed in claim 1. Although *Benson* teaches comparing linked directories, *Benson* does not teach granting any type of identifier based on the comparison of the directories. *Benson* teaches:

> When a user obtains access to the operating system using a system identifier and attempts to access a resource by using a resource-specific identifier, the operating system first determines whether the user (known to the system by a system identifier) is allowed to use the resource-specific identifier by comparing the linked directories. If the appropriate

> cross-reference between system identifier and resource-specific identifier is found, the operating system then determines the permission level for the resource-specific identifier.

Benson, column 2, lines 7-16.

Here, *Benson* describes an operating system comparing linked directories to determine a permission level for the user. However, *Benson* fails to teach "responsive to matching an entry in an access control list of a specific resource with credentials of a process, granting a security identifier given by the access control list to the process, wherein the security identifier has no meaning outside of being used to make an access decision for the specific resource," as is claimed in amended claim 1.

Independent claims 8, 15, and 22 recite similar features in their respective claim terminology. For example, amended claim 8 recites "granting means for granting a security identifier given by an access control list to a process in response to matching an entry in the access control list of a specific resource with credential of the process, wherein the security identifier has no meaning outside of being used to make an access decision for the specific resource." Therefore, claims 8, 15, and 22 are distinguishable over *Benson* for at least the reasons set forth above with regard to claim 1. Thus, *Benson* does not teach each and every feature of independent claims 1, 8, 15, and 22.

Moreover, at least by virtue of their dependency on independent claims 1, 8, and 15, the specific features of claims 2-7, 9-14, and 16-21 are not taught by *Benson*. Moreover, dependent claims 2-7, 9-14, and 16-21 recite additional combinations of features not taught by *Benson*. For example, dependent claims 2 recites "adding the security identifier to the credentials of the process to form an object access identifier, wherein the object access identifier is granted based on a path of execution." Dependent claims 9 and 16 recite similar subject matter. *Benson* teaches as follows:

> A flow chart of the secure access technique, using the exemplary designations shown in FIG. 2, is shown in FIG. 3. First, user1 requests access to system 1 at step 20 by entering a system identifier 2, SYSID1. The system checks system directory 3 to determine whether SYSID1 is a valid system identifier 2 on the system. If SYSID1 is not a valid system identifier, user1 is denied access to the system at step 22. If SYSID1 is a valid identifier, at step 24 user1 is required to pass a security test from security system 3 assigned for user1. If the security test is not passed, access to the system is denied at step 26. If the security test is passed, user1 is granted access to system 1 as SYSID1.

Benson, column 3, lines 48-58.

Here, *Benson* discloses checking a system directory to determine if a user's system identifier is valid. If the system identifier and a security test is passed, the user is granted access to the system. Again, *Benson* seems to assume that a user already has a system identifier. *Benson* does not teach granting a system identifier, a security identifier, or any other type of identifier to a user or a process. Moreover, *Benson* does not even mention adding the security identifier to the credentials of a process or

granting an identifier to a process based on a path of execution. Therefore, *Benson* fails to teach each and every limitation of claims 2, 9, and 16.

Claim 3 recites "adding the security identifier to the credentials of the process to form an object access identifier, wherein the object access identifier is granted based on an identity of the process and a second process invoked by the process." Claims 10 and 17 recite similar subject matter. *Benson* teaches checking a link between a system directory and a resource directory to determine if a user's system identifier has permission to access a resource rather than granting a security identifier to a process based on an identity of a process and a second process invoked by the process and adding the security identifier to the credentials of the process. For example, *Benson* states as follows:

> User1 next requests access to a resource 5, e.g., resource R1, at step 28. User1 enters her R1 resource-specific identifier 6a, e.g., R1ID1. System 1 checks the link between system directory 3 and resource directory 7a for R1 at step 30 to determine whether SYSID1 has permission to be resource identifier R1ID1 on resource R1. In one embodiment, this link is achieved using a cross-reference table that associates system identifiers with resource-specific identifiers found in the resource directories. *Benson,* column 3, lines 59-67.

As shown above, *Benson* teaches determining permission to access a resource based on a user's system identifier. *Benson* fails to teach granting a security identifier to a process based on an identity of the process and a second process invoked by the process, or any other criteria. Therefore, *Benson* fails anticipate claims 3, 10, and 17.

Finally, *Benson* fails to teach "comparing a second entry in the access control list with the credentials of the process; and responsive to the second entry matching the security identifier in the credentials of the process, generating an access decision that grants the process access to the specific resource, wherein the security identifier is a right in an access control list," as is recited in amended claim 7. As discussed above, *Benson* grants access to a resource based on a comparison of a user's system identifier with resource-specific identifiers in linked directories. *Benson* does not teach or even mention an access control list or comparing an entry in an access control list with a security identifier in the credentials of a process. Therefore, *Benson* fails to anticipate the features of claim 7. Consequently, it is respectfully urged that the rejection of claims 1-22 have been overcome. Therefore, Applicants respectfully request withdrawal of the rejection of claims 1-22 under 35 U.S.C. § 102.

Furthermore, *Benson* does not teach, suggest, or give any incentive to make the needed changes to reach the presently claimed invention. *Benson* actually teaches away from the presently claimed invention because it teaches a linked directory for comparing a system identifier with resource-specific identifiers as opposed to granting security identifier to a process that has no meaning outside of being used to make an access decision for the specific resource as in the presently claimed invention. Absent the examiner pointing out some teaching or incentive to implement *Benson* and a security identifier, one

of ordinary skill in the art would not be led to modify *Benson* to reach the present invention when the reference is examined as a whole. Absent some teaching, suggestion, or incentive to modify *Benson* in this manner, the presently claimed invention can be reached only through an improper use of hindsight using the applicants' disclosure as a template to make the necessary changes to reach the claimed invention.

III. Objection to Claims

The examiner has stated that claims 4, 11, and 18 were objected to because of the following informalities: recitation of an unnecessary article "a" in the claim language. In response, claims 4, 11, and 18 have been rewritten to overcome this objection. Therefore, Applicants request withdrawal of the objections.

IV. Conclusion

It is respectfully urged that the subject application is patentable over *Benson* and is now in condition for allowance.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: February 6, 2007

Respectfully submitted,

/Mari Ann Stewart/

Mari Ann Stewart
Reg. No. 50, 359
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants